POLYVERSE

Polyverse Microservice Firewall Solution Becomes Part of Docker Certification Program

Groundbreaking Cybersecurity Solution
Now Available on Docker Store

KIRKLAND, WA — MARCH 2 2017 — Polyverse Corporation, a rapidly growing cybersecurity company based in Kirkland, WA, today announced that its Microservice Firewall cybersecurity solution is now part of the Docker Certification Program, and available to customers on the Docker Store. The Polyverse Microservice Firewall uses advanced Moving Target Defense technology to dynamically reconfigure and adapt itself to a constantly changing cybersecurity landscape, offering peerless protection to microservices and Internet of Things networks.

"We would like to congratulate Polyverse on their acceptance into the Docker Certification Program," said Marianna Tessel, EVP, Strategic Development. "Enterprise IT teams are looking to Docker to provide recommendations and assurances on the ecosystem of container content, infrastructure and extensions. Polyverse's inclusion into the program indicates that its Microservice Firewall solution has been tested and verified by Docker, confirming for customers that its container images have been evaluated for security and are supported and built according to best practices."

Added Alexander Gounares, CEO of Polyverse, "Polyverse is extremely excited to join the Docker Certification Program, and delighted that our Microservice Firewall cybersecurity solution is now available to customers on the Docker Store."

A Radical New Approach to Cybersecurity

Hacking today's enterprise applications, systems and Internet of Things networks is a lot like playing lotto where the winning numbers are sitting in an unlocked drawer, just waiting to be stolen. No matter how sophisticated an organization's cyberdefenses, if its valuable systems are static and unchanging, cybercriminals will eventually breach them and take the jackpot.

Polyverse has built a cutting-edge cybersecurity solution that completely changes the game for cybersecurity, disrupting hackers' traditional advantages and eliminating the asymmetrical economic benefits of traditional hacking strategies. Our technologies:

- Rapidly cycle and return critical system applications to known good states every few seconds, automatically and pre-emptively removing any malware, even if it had otherwise gone undetected;
- Use compiler-based scrambling of an application's binary source code that effectively disables crafted zero-day exploits, even on unpatched systems. More valuably, scrambling provides inherent cyber-resiliency—no signature updates or cloud monitoring is required;
- Protect microservices and Internet of Things networks with a Microservice Firewall that dynamically configures itself to adapt to a constantly changing security landscape.

Polyverse's cybersecurity solution assumes that any application, service or connected device will inevitably be attacked and breached, so employs an advanced technology known as Moving Target Defense to continuously vary a target application's attack surface. Hackers are consequently confronted with a perplexing target that is constantly and randomly shifting.

For more about today's announcement, please contact Alex Gounares, Polyverse CEO, via (855) 765-9837 extension 700 or at alex@polyverse.io; or Andrew Vest, Director, Commercial Sales, via (855) 765-9837 extension 714 or at andrew@polyverse.io. For general information about Polyverse's cybersecurity solutions and to obtain a copy of our product overview, please visit https://polyverse.io.

All product and company names herein may be trademarks of their registered owners.